Nmap Scan Analysis

**Overview**

This document outlines the process and observations of a simple **Nmap** scan conducted for network analysis. Additionally, **Wireshark** was used to track packet flow during the scan.

**Scan Procedure**

**Step 1: Open Nmap**

Launch **Nmap** to begin the scanning process.

**Step 2: Open Terminal**

Access the terminal on your system to enter scanning commands.

**Step 3: Execute Basic Scan**

Run the following command for a **SYN scan**:

nmap -sS [IP Address]

This performs a stealthy SYN scan on the target system.

**Step 4: Advanced Scanning Options**

To refine results, additional **flags** can be used:

* **Aggressive Scan**: -A (Provides OS detection, version detection, and traceroute)
* **OS Scan**: -O (Attempts to determine the operating system)
* **Service Scan**: -sV (Identifies versions of running services)
* **IPv6 Scan**: -6 (Scans IPv6 addresses)

**Step 5: Packet Analysis with Wireshark**

Wireshark was used to track packets exchanged during the scan. Despite multiple approaches, no open ports were detected on the local network—meaning no services like **SSH, HTTP, or HTTPS** were accessible.

**Ethical Considerations**

* The scan was **NOT** conducted on unauthorized systems.
* **Scanme.org** was used as a test target.
* IPv6 address retrieval proved **unsuccessful**, reinforcing ethical boundaries for scanning external networks.

**Conclusion**

The scan confirmed that the tested network did not expose open ports. Wireshark provided valuable insights into packet behavior but did not uncover vulnerable services.